Solaris™ Security Toolkit 4.2 Release Notes

Sun Microsystems, Inc.
www.sun.com

Part No. 819-1504-10
July 2005, Revision A

Submit comments about this document at: http://www.sun.com/hwdocs/feedback

Copyright 2005 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A. All rights reserved.

Sun Microsystems, Inc. has intellectual property rights relating to technology that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more of the U.S. patents listed at http://www.sun.com/patents and one or more additional patents or pending patent applications in the U.S. and in other countries.

This document and the product to which it pertains are distributed under licenses restricting their use, copying, distribution, and decompilation. No part of the product or of this document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any.

Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and in other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, Java, AnswerBook2, docs.sun.com, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and in other countries.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and in other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

U.S. Government Rights—Commercial use. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Copyright 2005 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, Californie 95054, Etats-Unis. Tous droits réservés.

Sun Microsystems, Inc. a les droits de propriété intellectuels relatants à la technologie qui est décrit dans ce document. En particulier, et sans la limitation, ces droits de propriété intellectuels peuvent inclure un ou plus des brevets américains énumérés à http://www.sun.com/patents et un ou les brevets plus supplémentaires ou les applications de brevet en attente dans les Etats-Unis et dans les autres pays.

Ce produit ou document est protégé par un copyright et distribué avec des licences qui en restreignent l'utilisation, la copie, la distribution, et la décompilation. Aucune partie de ce produit ou document ne peut être reproduite sous aucune forme, par quelque moyen que ce soit, sans l'autorisation préalable et écrite de Sun et de ses bailleurs de licence, s'il y en a.

Le logiciel détenu par des tiers, et qui comprend la technologie relative aux polices de caractères, est protégé par un copyright et licencié par des fournisseurs de Sun.

Des parties de ce produit pourront être dérivées des systèmes Berkeley BSD licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays et licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, Java, AnswerBook2, docs.sun.com, et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays.

Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun™ a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une license non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciées de Sun qui mettent en place l'interface d 'utilisation graphique OPEN LOOK et qui en outre se conforment aux licences écrites de Sun.

LA DOCUMENTATION EST FOURNIE "EN L'ÉTAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFAÇON.

Contents

Preface vii

Solaris Security Toolkit 4.2 Release Notes 1

Changes for the Solaris Security Toolkit 4.2 Release 1

- Solaris 10 OS Support Changes 2
- Generic Changes 3

Solaris 10 OS Support Details 3

- New Framework Functions for Solaris Security Toolkit 4.2 Release 4
- New Scripts for Solaris Security Toolkit 4.2 Release 5
- Scripts Not Used for Solaris 10 OS 5
- New Environment Variables for Solaris Security Toolkit 4.2 Release 6
  - New Framework Variables 6
  - New Script Behavior Variables 6
- Environment Variables Not Used for Solaris 10 OS 7
- Functions Removed from Solaris Security Toolkit 4.2 Release 7
- `rpcbind` Automatically Disabled 7
- ▼ To Enable `rpcbind` 8

Supported SMS Versions 10

Solaris Security Toolkit Known Limitations 10

General Notes and Issues 10

Release Distributed Only in Package Format 10

SUNWjass and JASScustm Packages Are Now Relocatable 11

Solaris Security Toolkit and CTRL-C 11

Bugs in Solaris Security Toolkit 4.2 Software 11

When Using NIS, Multiple Reboots Might Result in Audit Errors (Bug ID 6222181) 11

Multiple Reboots Result in Uninitialized svcs and Audit Fail on nddconfig (Bug ID 6284872) 12

Bugs Affecting Solaris Security Toolkit 4.2 Software 12

Parameter for ip6_send_redirects Might Be Different Between Audits (Bug ID 6222001) 12

/etc/motd Should be Installed as a Volatile File (Bug ID 6222495) 13

svc.startd Misses Edge Case for optional_all (Bug ID 6223370) 13

Tables

TABLE 1 Solaris Security Toolkit Scripts Not Used for Solaris 10 OS 5

TABLE 2 Correlation Between SunOS and Solaris OS Versions 9

Preface

This document contains release notes for the Solaris™ Security Toolkit 4.2 software.

Before You Read This Book

This document is intended for the Solaris system administrator, who has a working knowledge of UNIX® systems, particularly those based on the Solaris Operating System (Solaris OS). If you do not have such knowledge, read the Solaris User and System Administrator documentation and consider UNIX system administration training.

Using UNIX Commands

This document might not contain information on basic UNIX commands and procedures such as shutting down the system, booting the system, and configuring devices. Refer to the following for this information:

- Software documentation that you received with your system
- Solaris Operating System documentation, which is at

  http://docs.sun.com

Shell Prompts

Shell	Prompt
C shell	*machine-name*%
C shell superuser	*machine-name*#
Bourne shell and Korn shell	$
Bourne shell and Korn shell superuser	#

Typographic Conventions

Typeface*	Meaning	Examples
AaBbCc123	The names of commands, files, and directories; on-screen computer output	Edit your .login file. Use ls -a to list all files. % You have mail.
AaBbCc123	What you type, when contrasted with on-screen computer output	% **su** Password:
AaBbCc123	Book titles, new words or terms, words to be emphasized. Replace command-line variables with real names or values.	Read Chapter 6 in the *User's Guide*. These are called *class* options. You *must* be superuser to do this. To delete a file, type rm *filename*.

* The settings on your browser might differ from these settings.

Related Documentation

The documents listed as online are available at:

http://www.sun.com/products-n-solutions/hardware/docs/Software/enterprise_computing/systems_management/sst/index.html

Application	Title	Part Number	Format	Location
Reference	*Solaris Security Toolkit 4.2 Reference Manual*	819-1503-10	PDF HTML	Online
Administration	*Solaris Security Toolkit 4.2 Administration Guide*	819-1402-10	PDF HTML	Online
Man Pages	*Solaris Security Toolkit 4.2 Man Page Guide*	819-1505-10	PDF	Online

Documentation, Support, and Training

Sun Function	URL	Description
Documentation	http://www.sun.com/documentation/	Download PDF and HTML documents, and order printed documents
Support	http://www.sun.com/support/	Obtain technical support and download patches
Training	http://www.sun.com/training/	Learn about Sun courses

Third-Party Web Sites

Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. You can submit your comments by going to:

http://www.sun.com/hwdocs/feedback

Please include the title and part number of your document with your feedback:

Solairs Security Toolkit 4.2 Release Notes, part number 819-1504-10

Solaris Security Toolkit 4.2 Release Notes

This guide contains release notes for the 4.2 release of the Solaris™ Security Toolkit software, also known as JumpStart™ Architecture and Security Scripts (JASS), and contains the following topics:

- Changes for the Solaris Security Toolkit 4.2 Release
- Solaris 10 OS Support Details
- Supported Hardware Systems
- Supported Solaris OS Versions
- Supported SMS Versions
- Solaris Security Toolkit 4.2 Known Limitations
- General Notes and Issues
- Bugs in Solaris Security Toolkit 4.2 Software
- Bugs Affecting Solaris Security Toolkit 4.2 Software

Changes for the Solaris Security Toolkit 4.2 Release

This section of the release notes describes the major changes that have been made for the Solaris Security Toolkit 4.2 software release. For more information and details about those changes, refer to the *Solaris Security Toolkit 4.2 Reference Manual*.

Note – The `CHANGES` file that was supplied with the `Documentation` directory in previous releases of the Solaris Security Toolkit software is no longer supplied. Instead the changes are recorded in this document.

Solaris 10 OS Support Changes

This Solaris Security Toolkit 4.2 software release provides support for the Solaris 10 Operating System (OS).

Using the Solaris Security Toolkit 4.2 software, you can harden and audit the security of systems in a similar manner as earlier versions. You can also use this release of software either in JumpStart or standalone mode, as in earlier versions.

Following are the major changes made for this release to support the Solaris 10 OS. See Solaris 10 OS Support Details for more information.

- SMF-Ready Services - provides the capability for many Solaris Security Toolkit scripts to use the Service Management Facility (SMF) services interface, the Fault Management Resource Identifiers (FMRIs), and the start and stop scripts.
- Legacy Services - provides the capability for SMF to recognize as legacy services some of the Solaris Security Toolkit scripts that are not SMF-ready.
- Zones - provides the capability to harden and audit zones in the Solaris 10 OS.
- TCP Wrappers - provides Transmission Control Protocol (TCP) Wrappers configurations for Solaris Security Toolkit drivers.
- MD5 - provides support of the Solaris 10 OS message_digest 5 (`md5`) algorithm functionality through the `digest -a md5` command, which renders the `SUNBEmd5` package unnecessary on Solaris 10 OS systems.
- Manage Routing - provides new scripts to manage routing in the Solaris 10 OS.
- New Home Root Directory - provides a new home root directory of `/root` instead of the standard `/` for the root directory.
- IP Filter - provides an integrated firewall capability through integration of the freeware Internet Protocol (IP) Filter.
- BART - provides support for the Basic Audit Reporting Tool (BART), which enables you to determine file-level changes that have occurred on your systems, among other functions.
- Flexible Crypt - provides support for using several new tunables in the Solaris 10 OS, which control the algorithms used for password encryption.
- Account Locking - provides support for the Solaris 10 OS ability to lock an account after a pre-defined set of failed login attempts.
- Parameterized Password Checking - provides support for the Solaris 10 OS strict password checking.
- Password History - provides support for password safety checks that have been added to the Solaris 10 OS.
- RPC BIND - provides support for disabling or enabling the Remote Procedure Call from the Berkeley Internet Name Domain (rpcbind).
- Perl - provides support for creating Solaris Security Toolkit scripts in the Practical Extraction and Report Language (Perl) for use with the Solaris 10 OS.

- XFS - provides support for disabling or enabling the X Font Server. XFS clients connect to the server to request a font set, and the server reads the font files from the disk and serves them to the clients. The X Font Server daemon is managed by the SMF.
- GNOME - provides support for disabling or enabling support for GNU Network Object Model Environment (GNOME) as well as the Common Development Environment (CDE).

Generic Changes

In addition to the changes made for this release to support the Solaris 10 OS, the following generic changes have also been made for this release:

- Relocatable Package - provides a relocatable Solaris Security Toolkit 4.2 package, so that it can be installed to whatever directory you want by using the correct options to the `pkgadd` command.
- Removing Backup Files - provides the capability to remove Solaris Security Toolkit backup files
- Combining Driver Functionality - incorporates the functionality of the `desktop-{secure|config|hardening}.driver`, `sunfire_15k_domain-{secure|config|hardening}.driver`, and `jumpstart-{secure|config|hardening}.driver` into `server-{secure|config|hardening}.driver`
- Intelligent Defaults - provides support for intelligent defaults; that is, allows the user to press Return to specify a default where feasible.
- Verbosity - supports reduced verbosity output for `jass-execute` and `jass-check-sum` commands.
- `IIim` - provides support for disabling and enabling the Internet-Intranet Input Method (`IIim`), which handles Asian input for Solaris OS software.
- Consistent Return Values and Help Output - provides consistent return values and help output for all Solaris Security Toolkit commands.
- Apache 2 - provides support for `apache2`.

Solaris 10 OS Support Details

The following section contains some further details of Solaris 10 OS support changes in this release.

New Framework Functions for Solaris Security Toolkit 4.2 Release

The following functions are new in this release and can be used only on systems running the Solaris 10 OS. Functions are explained in Chapter 2 of the *Solaris Security Toolkit 4.2 Reference Manual*.

These common log functions were added to Solaris Security Toolkit 4.2 software:

- `logNotGlobalZone`
- `logScore`
- `logScriptFailure`
- `logServiceDisabled and logServiceEnabled`
- `logServiceInstalled` and `logServiceNotInstalled`
- `logServiceOptionDisabled` and `logServiceOptionEnabled`
- `logServiceProcessList`
- `logServicePropDisabled` and `logServicePropEnabled`
- `logServiceRunning` and `logServiceNotRunning`
- `logUserLocked` and `logUserNotlocked`
- `logUndoBackupWarning`

These common miscellaneous functions were added to Solaris Security 4.2 software:

- `get_driver_report`
- `get_lists_conjunction`
- `get_lists_disjunction`

These public driver functions were created to support SMF in the Solaris Security Toolkit 4.2 framework:

- `add_option_to_ftpd_property`
- `change_group`
- `change_mode`
- `change_owner`
- `check_serviceDisabled`
- `check_serviceEnabled`
- `check_serviceInstalled`
- `check_serviceNotInstalled`
- `check_serviceNotRunning`
- `check_serviceOptionEnabled`
- `check_servicePropDisabled`
- `check_serviceRunning`
- `check_serviceOptionDisabled`
- `check_userLocked`
- `check_userNotLocked`
- `convert_inetd_service_to_fmri`
- `disable_service`
- `enable_service`
- `is_service_enabled`

- is_service_installed
- is_service_running
- is_user-account_extant
- is_user_account_locked
- is_user_account_login_not_set
- lock_user_account
- make_link
- set_service_property_value
- set_stored_keyword_val
- unlock_user_account
- update_inetcon_in_upgrade

New Scripts for Solaris Security Toolkit 4.2 Release

Following are the new finish and audit scripts for the Solaris Security Toolkit 4.2 release. The functions of finish (`.fin`) scripts are explained in Chapter 5 of the *Solaris Security Toolkit 4.2 Reference Manual*, and the functions of audit (`.aud`) scripts are explained in Chapter 6 of the *Solaris Security Toolkit 4.2 Reference Manual*.

- `disable-apache2.{fin|aud}`
- `disable-appserv.{fin|aud}`
- `disable-IIim.{fin|aud}`
- `disable-routing.{fin|aud}`
- `enable-account-lockout.{fin|aud}`
- `enable-bart.{fin|aud}`
- `enable-ipfilter.{fin|aud}`
- `enable-password-history.{fin|aud}`
- `set-root-home-dir.{fin|aud}`
- `set-strict-password-checks.{fin|aud}`

Scripts Not Used for Solaris 10 OS

lists the Solaris Security Toolkit scripts that are not used when you are hardening the Solaris 10 OS.

TABLE 1 Solaris Security Toolkit Scripts Not Used for Solaris 10 OS

Script Name	Applicable Operating System
`disable-ab2`	Solaris 2.5.1 through 8
`disable-aspp`	Solaris 2.5.1 through 8
`disable-picld`	Solaris 8 and 9

TABLE 1 Solaris Security Toolkit Scripts Not Used for Solaris 10 OS *(Continued)*

Script Name	Applicable Operating System
install-fix-modes	Solaris 2.5.1 through 9
install-newaliases	Solaris 2.5.1 through 8
install-openssh	Solaris 2.5.1 through 8
install-sadmind-options	Solaris 2.5.1 through 9
install-strong-permissions	Solaris 2.5.1 through 9
remove-unneeded-accounts	Solaris 2.5.1 through 9

New Environment Variables for Solaris Security Toolkit 4.2 Release

This section lists the framework and script behavior environment variables that are new in this release and can be used only on systems running the Solaris 10 OS. The functions of environment variables are explained in Chapter 7 of the *Solaris Security Toolkit 4.2 Reference Manual*.

New Framework Variables

- JASS_DISPLAY_HOST_LENGTH
- JASS_DISPLAY_SCRIPT_LENGTH
- JASS_DISPLAY_TIME_LENGTH
- JASS_FILE_COPY_KEYWORD
- JASS_ROOT_HOME_DIR
- JASS_RUN_CLEAN_LOG
- JASS_RUN_VALUES
- JASS_SAVED_BACKUP
- JASS_SCRIPT
- JASS_SCRIPT_FAIL_LOG
- JASS_SCRIPT_NOTE_LOG
- JASS_SCRIPT_WARN_LOG
- JASS_UNDO_TYPE

New Script Behavior Variables

- JASS_CRYPT_ALGORITHMS_ALLOW
- JASS_CRYPT_ALGORITHMS_DEFAULT
- JASS_CRYPT_DEFAULT
- JASS_CRYPT_FORCE_EXPIRE

- JASS_PASS_DICTIONLIST
- JASS_PASS_DICTIONDBDIR
- JASS_PASS_HISTORY
- JASS_PASS_MAX_REPEATS
- JASS_PASS_MIN_ALPHA
- JASS_PASS_MINDIFF
- JASS_PASS_MINDIGIT
- JASS_PASS_MINLOWER
- JASS_PASS_MINNONALPHA
- JASS_PASS_MINSPECIAL
- JASS_PASS_MINUPPER
- JASS_PASS_NAMECHECK
- JASS_PASS_WHITESPACE
- JASS_ZONE_NAME

Environment Variables Not Used for Solaris 10 OS

The following environment variables are *not* used for the Solaris 10 OS:

- JASS_ISA_CAPABILITY (*removed from Solaris Security Toolkit 4.2 software*)
- JASS_DISABLE_MODE

Functions Removed from Solaris Security Toolkit 4.2 Release

The files and scripts relating to the following functions have been removed from the Solaris Security Toolkit 4.2 software as they are no longer needed:

- Installing the misc/klmmod kernel module on domains for Sun Fire high-end systems
- Installing the Sun ONE Web Server
- sunfire_mf_msp-{secure|config|hardening}.driver
- 32-bit functionality
- Sun Enterprise™ 1000 (Starfire™), as the product is now at end of life.

rpcbind Automatically Disabled

The secure.driver and the sunfire-15k_sc-secure.driver in the Solaris Security Toolkit 4.2 software disabled rpcbind as previous versions of the toolkit have done. However, in the Solaris 10 OS, there are services which depend on

rpcbind such as Network Information Services (NIS), the Network File System (NFS), and window managers, such as the Common Desktop Environment (CDE), and the GNU Network Object Model Environment (GNOME). By default, the configuration of the secure.driver and the sunfire-15k_sc-secure.driver disabled these services, so you must enable rpcbind to use them.

Note – The server-secure.driver and the suncluster3x-secure.driver do *not* disable rpcbind.

▼ To Enable rpcbind

1. **Unharden the system.**
2. **Copy and rename the** secure.driver **and** hardening.driver **to** *new-secure.driver* **and** *new-hardening.driver*, **where** *new-secure.driver* **is the name you choose for your new customized** secure.driver**, and** *new-hardening.driver* **is the name you choose for your new customized** hardening.driver**.**
3. **Edit** *new-secure.driver* **to replace the reference to** hardening.driver **with** *new-hardening.driver***.**
4. **Comment out the** disable-rpc.fin **script from** *new-hardening.driver***.**
5. **Re-run hardening with your customized copy drivers by running the Solaris Security Toolkit with** *new-secure.driver***.**
6. **Reboot the system.**

Caution – After enabling the rpcbind service, additional services may be started automatically and their corresponding ports opened. The Solaris Security Toolkit audit flags these additional services as failures.

Supported Hardware Systems

Solaris Security Toolkit 4.2 software supports SPARC®, 64-bit *only*, and x86 systems.

Supported Solaris OS Versions

Sun support for Solaris Security Toolkit software is available only for its use in the Solaris 8, Solaris 9, and Solaris 10 Operating Systems.

Note – For Solaris Security Toolkit 4.2 software, the Solaris 10 OS can be used *only* on Sun Fire high-end systems domains, *not* on the system controller (SC).

While the software can be used in the Solaris 2.5.1, Solaris 2.6, and Solaris 7 Operating Systems, Sun support is not available for its use in those operating systems.

The Solaris Security Toolkit software automatically detects which version of the Solaris Operating System software is installed, then runs tasks appropriate for that operating system version.

You will note in examples provided throughout this document that when a script checks for a version of the OS, it checks for 5.*x*, the SunOS™ versions, instead of 2.*x*, 7, 8, 9, or 10, the Solaris OS versions. shows the correlation between SunOS and Solaris OS versions.

TABLE 2 Correlation Between SunOS and Solaris OS Versions

SunOS Version	Solaris OS Version
5.5.1	2.5.1
5.6	2.6
5.7	7
5.8	8
5.9	9
5.10	10

Supported SMS Versions

If you are using System Management Services (SMS) to run the system controller (SC) on your Sun Fire high-end systems, then Solaris Security Toolkit 4.2 software is supported on all Solaris 8 and 9 OS versions when used with SMS versions 1.4, 1.4.1, and 1.5. No version of SMS is supported on Solaris 10 OS with Solaris Security Toolkit 4.2 software.

Note – For Solaris Security Toolkit 4.2 software, the Solaris 10 OS can be used *only* on domains, *not* on the system controller (SC).

Solaris Security Toolkit Known Limitations

This section contains known limitations for the Solaris Security Toolkit 4.2 software:

- While the Solaris Security Toolkit 4.2 software maintains its functionality for disabling system accounts (see the finish script `disable-system-accounts.fin`), it no longer modifies the system to record login attempts to those disabled accounts.

General Notes and Issues

This section contains general notes and issues that involve the Solaris Security Toolkit 4.2 software.

Release Distributed Only in Package Format

The Solaris Security Toolkit 4.2 release is distributed *only* in package format.

SUNWjass and JASScustm Packages Are Now Relocatable

As of this Solaris Security Toolkit 4.2 release, the SUNWjass and JASScustm packages are relocatable, making them consistent with Sun's packaging standards. You can relocate these packages using the pkgadd(1M) -R command.

Solaris Security Toolkit and CTRL-C

Performing a CTRL-C during Solaris Security Toolkit hardening and undo operations could result in an inconsistent system state. Hardening operations should be allowed to complete and then a subsequent undo operation performed instead of interrupting the hardening operation. Do *not* use CTRL-C for error handling or to interrupt a toolkit run. Wait until the operation has finished and then re-perform hardening or undo operations.

Bugs in Solaris Security Toolkit 4.2 Software

This section summarizes the bugs that you might encounter that have *not* been fixed in the Solaris Security Toolkit 4.2 software.

When Using NIS, Multiple Reboots Might Result in Audit Errors (Bug ID 6222181)

rpcbind is disabled by default in the secure.driver. If you are using NIS, there are circumstances where rebooting the system leaves all the services that are normally started by inetd in an uninitialized state and legacy services do not work. This shows in the Solaris Security Toolkit as a discrepancy between audit results from before and after a reboot, in services started by inetd.

This bug will be fixed by the Solaris 10 OS Bug ID 6223370. See description of this bug in "Bugs Affecting Solaris Security Toolkit 4.2 Software."

Workarounds:

- If you want to use NIS, enable rpcbind and reboot. Refer to Chapter 1 of the *Solaris Security Toolkit 4.2 Reference Manual*.

- If you do *not* want to use NIS, disable NIS. (Refer to the Solaris 10 OS naming service document for how to disable NIS.)

Multiple Reboots Result in Uninitialized `svcs` and Audit Fail on `nddconfig` (Bug ID 6284872)

Multiple reboots after hardening result in `svcs` being uninitialized, and the audit to fail on `nddconfig`. In other words, the `nddconfig` audit will *not* contain zero errors after the system reboots multiple times.

The problem is that `milestone/name-services` is not able to come online with `rpcbind` disabled and the system configured to use NIS. Because of this, the `/etc/rc2.d (svc:/milestone/multi-user:default)` does not run, and so the `nddconfig` script does not run.

This bug will be fixed by the Solaris 10 OS Bug ID 6223370.

Workarounds:

- If you want to use NIS, enable `rpcbind` and reboot. Refer to Chapter 1 of the *Solaris Security Toolkit 4.2 Reference Manual*.
- If you do *not* want to use NIS, disable NIS. Refer to the Solaris 10 OS naming service document for how to disable NIS.

Bugs Affecting Solaris Security Toolkit 4.2 Software

This section summarizes the bugs that you might encounter that have *not* been fixed in other software that affects the Solaris Security Toolkit.

Parameter for `ip6_send_redirects` Might Be Different Between Audits (Bug ID 6222001)

This Solaris 10 OS bug could affect your operation of Solaris Security Toolkit 4.2 software. Sometimes you might see a different parameter for `ip6_send_redirects` between audits, where it should be the same. For example, you might audit a system that has not been hardened (Audit #1). Then you harden the system, reboot, undo the hardening, and reboot. You audit the system again (Audit #2).

You would expect to see identical audit results except for the timestamp. However, sometimes, you might see a difference in the `ip6_send_redirects` parameter in the `nddconfig` file between the first and second audit. In the first audit, the message says the check failed because the parameter is not 0. In the second audit, the message says the check passed because the parameter is 0, which is the correct response.

Workaround: None

`/etc/motd` Should be Installed as a Volatile File (Bug ID 6222495)

This Solaris 10 OS bug could affect your operation of Solaris Security Toolkit 4.2 software. The file `/etc/motd` is delivered by the `SUNWcsr` package with a file type of `f`. The Solaris Security Toolkit 4.2 drivers replace this file, which can lead to errors and warnings when installing zones and packages within zones.

Workarounds:

You can do one of the following:

- Remove the file from the `JASS_FILES` list, so it is *not* installed.
- Modify the file type to `v` to remove this error.

`svc.startd` Misses Edge Case for `optional_all` (Bug ID 6223370)

If you disable `rpcbind` and reboot, `milestone/name-services` do *not* come online, which might cause `inetd` and other services *not* to come online. For several ways this Solaris 10 OS bug could affect your operation of Solaris Security Toolkit 4.2 software, see descriptions of Bug ID 6284872 and Bug ID 6222181.

Workarounds:

- If you want to use NIS, enable `rpcbind` and reboot. Refer to Chapter 1 in the Solaris Security Toolkit 4.2 Reference Manual.
- If you do not want to use NIS, disable NIS. Refer to the Solaris 10 OS naming service document for how to disable NIS.